InfoSec prerequisites to become a Pentester/Hacker or a Bug Bounty Hunter

By: Aayan

CISSP:

You don’t have to become a master in it to Cr4ck it’s exam but if even you want to! No problem go ahead focus on it and have good understanding of it’s 8 domains explaination about Cyber security.

#way to learn:

Read the book of shon haris all in one cissp 8th edition, read articles on medium which people are sharing their ways how to pass it’s exam easily.

It will help you to understand the world of CISSP as it is inch deep and mile wide course. It’s full of theory, have a cup of tea/coffee and keep reading. Have rest when you feel tired of reading it, do not force yourself to read 5 more pages you won’t remember what you have read in those 5 pages. And it is worth it to understand:

Note: In CISSP you are an advicer not a problem solver.

Book: https://pk1lib.org/book/3644814/23491d

Operating Systems(OS):

Understanding operating systems is the next essential thing, to become a h4ck3r you must understand how a system works more than knowing to use it. First of all understand the core system how a an operating system works how it interacts with hardware, search on google there are many short explanations about UNIX/Linux and windows.

In linux You should understand how(Command line interface) works how the behind console works, understand the boot process file management Bash scripting etc. Practice on ubuntu Lts whether Mint.

In windows all you have to learn is sysinternals **Note**:Do not go in depth in it. Aside that learn powershell scripting and how it can be used same as Linux bash fish shells etc.

Book linux: https://pk1lib.org/book/11771389/fe6ae8
Book Windows: https://pk1lib.org/book/3570960/37b0a9

Note: You don’t have to go in-depth for windows it’s optional, Otherwise short articles are enough on google about internals.

Networking:

Here it comes! Learning networking is really important because there's nothing possible without networking **Protocols**, you must learn TCP/IP, HTTP, DHCP, ICMP, NAT, ARP, etc. you must learn and understand each lecture of CompTia network plus.

There is CCNA but not needed nor it's essential you just need to focus on network plus learn all protocols specially tcp/ip how tcp 3 way handshake works Ip subnetting different classes of Ip, Private and Public addresses.

After that you must take that knowledge to little further, learn wireshark and intercept/monitor packets, capture in-coming and out-going traffic when you are surfing web whether you are using a software connected with internet. You can read RFC documents written by Network engineers simply search on google.

Resources: https://www.youtube.com/watch?v=IErQm8wsaxg&list=PL_YW0h4ytNBtBBaPFgMzCNmnzlFalu-SA

https://www.youtube.com/watch?v=NjvR4LmwcMU&list=PLBf0hzazHTGPgyxeEj_9LBHiqjtNEjsgt

https://www.youtube.com/watch?v=5MTZdN9TEO4&list=PLBf0hzazHTGM8V_3OEKhvCM9Xah3qDdIx

Hardware Concepts (Basics):

Understanding (Architecture) hardware concepts are key things, it will help you to learn Buffer overflows, exploit development, binary exploitation, memory heap spray etc.

Learn about CPU and RAM how they both work together, learning ARM and x86_64 assembly lanuages are **optional** but if you learn these will make you a M4st3r as these are low-level languages and really closer to Hardware.

Learning basic C/C++ is really helpful to learn assembly, and it will be helpful to master python aswell as it is high-level language it's easy to learn than c/c++ but learning c/c++ first would be helpful because you'll lose strength for c/c++ if you will learn python first.

Computer Architecture Book: https://pk1lib.org/book/1264055/5fff3f

C/C++: https://www.youtube.com/playlist?list=PLu0W_9lII9aiXlHcLx-mDH1Qul38wD3aR

Python,Html,Js,Php:

You must have learned basics of C/C++,

now it’s time to learn high level languages to take your skills further in your journey, learning python is not just helpful but it’s a superpower language as it has many libraries of exploitation, networking, machine learning, deep learning etc. And it will be help because you’ll be automating your hacking/e-exploitation process.

After that learn Html,Js and php majority of webistes written in these languages, ofcourse there are many other languages but to become a web pentester/Bug hunter you don’t need to become a web developer, aswell learning web technologies is essential and key thing.

Resource: https://www.youtube.com/watch?v=gfDE2a7MKjA&t=33920s

for Html,Js,Php and technologies

Website: developer.mozilla.org

Hacking journey:

Once you have learned basics you should start learning hacking/pentesting, First of all you must have understanding of security concepts and different cyber Attacks, and for that you must learn CompTia Security Plus.

After that do not waste your time on different un-valuable websites just go to INE site and complete your eJPT (Junior penetration tester) course as it covers basics to somewhat intermediate, once you have hacker mindset after this course.

You can prepare for Offsec PWK exploiting machines on tryhackme vulnhub and hackthebox:

I'm gonna add some Youtube channels names which will teach you System/network and Web pentesting/bug bounties.
Good luck Fellas believe me there's a lot bounties you can hunt, you can even learn by freelancing and last thing If you learn Machine learning and use it in Offensive security you can bring down M0nst3rs.

And remember one of also the best way of learning hacking is by solving **CTF** challenges.

Websites:

CTFlearn (site)
PicoCTF (site)
ine.com
tryhackme (site)
portswigger (site)
hackthebox (site)
OWASP (site)
VulnHub (site)

Youtube:

For security plus search (syo-601 messor)
Null-byte (Channel)
Networkchuck (Channel)
Cybermentor (Channel)
Liveoverflow (One of my Fav Channel)